OFFICE OF THE DIRECTOR
DEFENSE RESEARCH AND ENGINEERING
3040 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-3040

October 31, 2000

MEMORANDUM FOR DIRECTORS SHARED RESOURCES

SUBJECT: Kerberos and SecurID Authentication

The High Performance Computing Modernization Program (HPCMP) must maintain a strong security posture in response to real world security threats. The HPCMP requirement to access all HPCMP unclassified resources using Kerberos with SecurID authentication is an integral component of our security posture.

The use of traditional UNIX static passwords adds unnecessary risk and is subject to a variety of hostile attacks. To mitigate those risks, Kerberos with SecurID authentication must be used instead of traditional UNIX passwords for accessing HPCMP resources. The HPCMP Shared Resource Centers have been directed to implement Kerberos and SecurID as described by the HPCMP Security Implementation Group Kerberos/Passcode/Secure Shell Implementation White Paper on all unclassified SRC systems.

I will consider temporary waivers to this requirement under certain limited conditions. Waivers may be appropriate for non-production efforts associated with product evaluations, test-beds, or tests of alternate hardware pre-authentication. Systems receiving waivers must be hardened and placed on a seperate well-protected network segment, i.e., distinct from the rest of the shared resource center's local area network and incorporating a firewall of filtering router. An additional Site Assistance Visit (SAV) and/or Security Test and Evaluation (ST&E) may be required to ensure the security of HPCMP resources.

Points of contact (POC) for this action will be Mr. Steve Schneller, SchnellerSA@Npt.NUWC.Navy.Mil, 410-832-3820; Mr. Joe Molnar, molnar@hpcmo.hpc.mil or Mr. Doug Butler, dbutler@hpcmo.hpc.mil. Mr. Butler and Mr. Molnar can be reached at 703-812-8205.

[signed]

CRAY J. HENRY
Director
High Performance Computing
Modernization Program